Data Security

Lect. 5

Cryptography and Network Security Chapter 6

Fifth Edition

by William Stallings

Multiple Encryption & DES

- clear a replacement for DES was needed
  - theoretical attacks that can break it
  - demonstrated exhaustive key search attacks
- AES is a new cipher alternative
- prior to this alternative was to use multiple encryption with DES implementations
- Triple-DES is the chosen form

Why not Double-DES?

- could use 2 DES encrypts on each block
  - $C = E_{K2}(E_{K1}(P))$
- concern at time of reduction to single stage
- "meet-in-the-middle" attack
  - works whenever use a cipher twice
  - since $X = E_{K1}(P) = D_{K2}(C)$
  - attack by encrypting P with all keys and store
  - then decrypt C with keys and match X value
  - can show takes $O(2^{56})$ steps
  - Requires… known plaintext

Triple-DES with Two-Keys

- hence must use 3 encryptions
  - would seem to need 3 distinct keys
- but can use 2 keys with E-D-E sequence
  - $C = E_{K1}(D_{K2}(E_{K1}(P)))$
  - if $K1=K2$ then can work with single DES
- standardized in ANSI X9.17 & ISO8732
- no current known practical attacks
  - several proposed impractical attacks might become basis of future attacks.

Triple-DES with Three-Keys

- although are no practical attacks on two-key Triple-DES have some indications
- can use Triple-DES with Three-Keys to avoid even these
  - $C = E_{K3}(D_{K2}(E_{K1}(P)))$
- has been adopted by some Internet applications, e.g., PGP, S/MIME

Modes of Operation

- block ciphers encrypt fixed size blocks
  - e.g., DES encrypts 64-bit blocks
- need some way to en/decrypt arbitrary amounts of data in practice
- NIST SP 800-38A defines 4 modes
- have **block** and **stream** modes
- to cover a wide variety of applications
- can be used with any block cipher

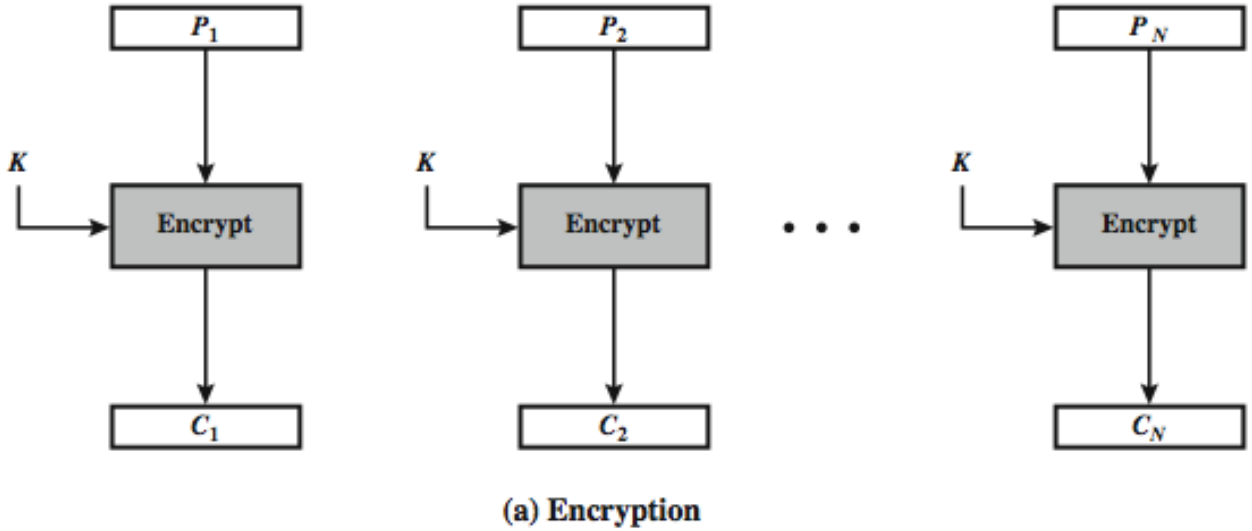
Electronic Codebook Book (ECB)

- message is broken into independent blocks that are encrypted
- each block is a value which is substituted, like a codebook, hence name
- each block is encoded independently of the other blocks

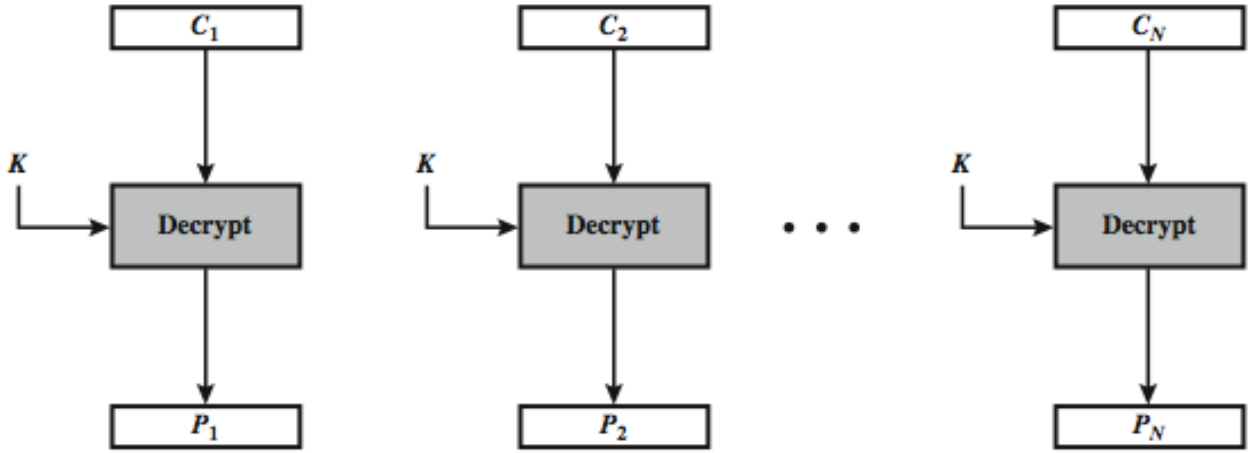
$$C_i = E_K(P_i)$$

- Applications (uses): secure transmission of single values or sending a few blocks of data(single values as an encryption key).

Electronic Codebook Book (ECB)



(a) Encryption



(b) Decryption

Advantages and Limitations of ECB

- message repetitions may show in ciphertext
- weakness is due to the encrypted message blocks being independent.
- Advantage: a problem in encryption or decryption of a block doesn't affect other blocks- an error in one block isn't propagated in other blocks -if one or more bits are corrupted during transmission, it only affects the bits in the corresponding plaintext after decryption, other plaintext blocks are not affected.

Advantages and Limitations of ECB

- If one or more bits are corrupted during transmission , it only affects the bits in the corresponding plaintext after decryption other plaintext blocks are not affected.
- This is an advantage for noisy channel
- Applications: Secure transmission of single values as an encryption key.
- For lengthy messages, the ECB mode may not be secure: if the message is highly structured, it may be possible for attacker to exploit these regularities.

Cipher Block Chaining (CBC)

- It tries to overcome some of the problems in the problems in ECB by including the previous cipher block in the preparation of the current block.
- message is broken into blocks.
- linked together in encryption operation
- each previous cipher block is chained with current plaintext block, hence name
- use Initial Vector (IV) to start process

Cipher Block Chaining (CBC)

- When a block is completely encrypted, the block is sent, but a copy of it is kept in a register to be used for encryption of the next block.
- use Initial Vector (IV) to start process

$C_i = E_K(P_i \text{ XOR } C_{i-1})$

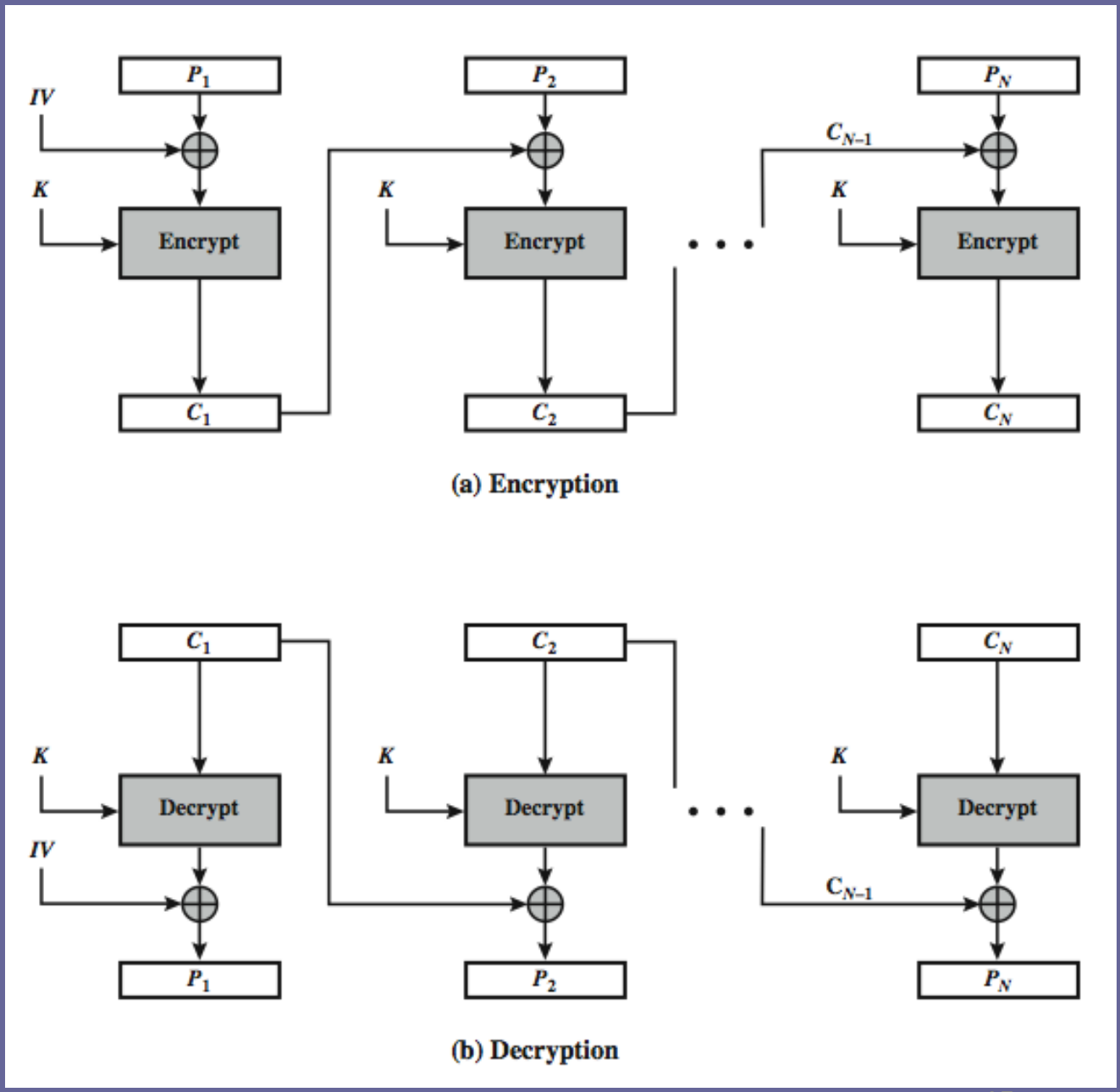
$C_0 = IV$ initial value –both the sender and the receiver agree upon.

- IV prevents same P from making same C
- uses: bulk data encryption, authentication

Cipher Block Chaining (CBC)

- Blocks are dependent on each other.
- Disadvantages: encryption of a block affects other blocks. The error in one block is propagated to the other blocks.

Cipher Block Chaining (CBC)



Message Padding

- at end of message must handle a possible last short block
  - which is not as large as blocksize of cipher
  - pad either with known non-data value
    - e.g., nulls
  - or pad last block along with count of pad size
    - e.g., [b1 b2 b3 0 0 0 0 5]
    - means have 3 data bytes, then 5 bytes pad+count
  - this may require an extra entire block over those in message
- there are other, more esoteric modes, which avoid the need for an extra block

Advantages and Limitations of CBC

- a ciphertext block depends on **all** blocks before it
- any change to a block affects all following ciphertext blocks... avalanche effect
- need **Initialization Vector** (IV)
  - which must be known to sender & receiver

Stream Modes of Operation

- block modes encrypt entire block
- may need to operate on smaller units
  - real time data
- convert block cipher into stream cipher
  - cipher feedback (CFB) mode
  - output feedback (OFB) mode
  - counter (CTR) mode
- use block cipher as some form of **pseudo-random number** generator... Vernam cipher

Cipher FeedBack (CFB)

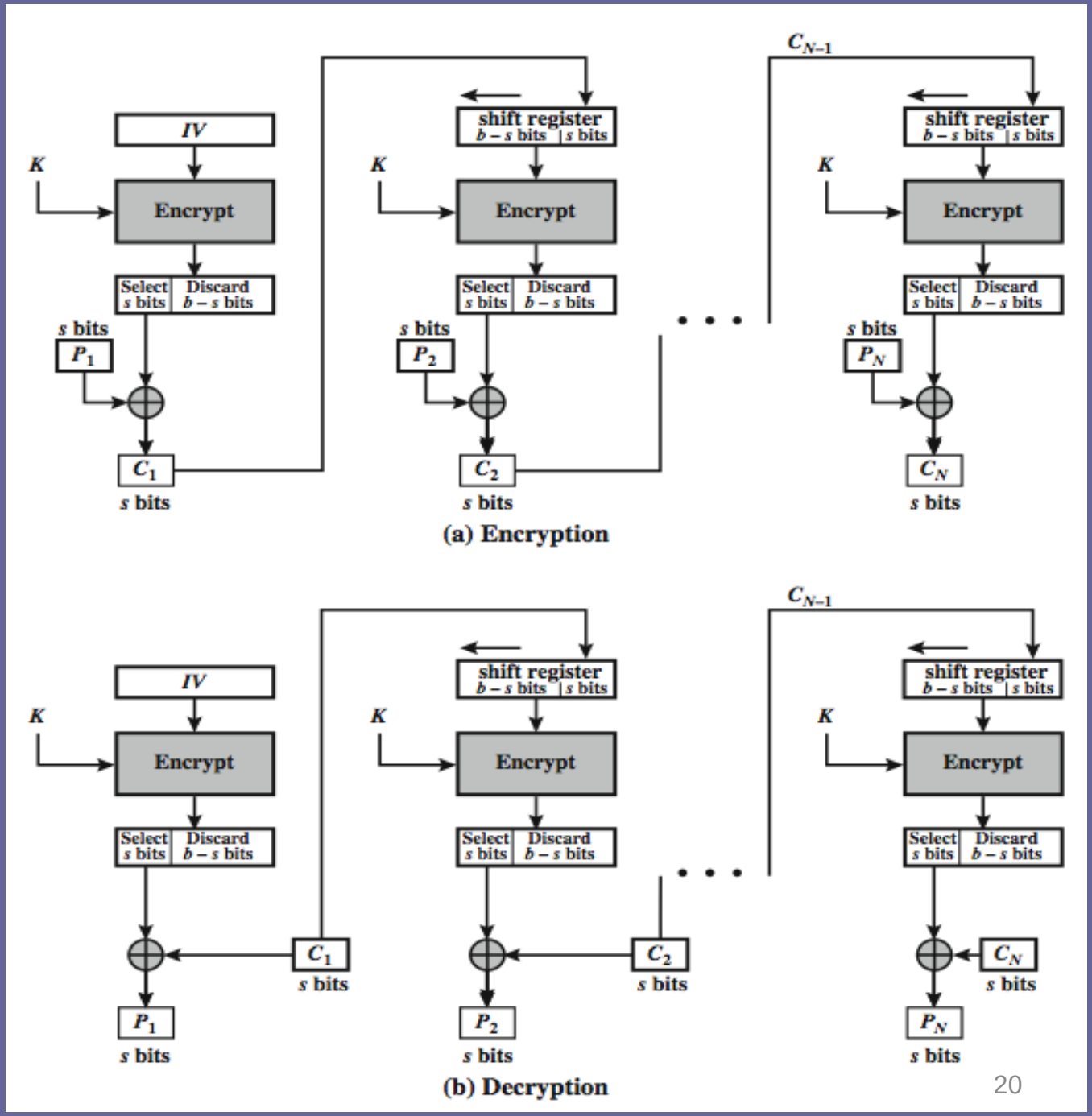
- message is treated as a stream of bits
- added to the output of the block cipher
- result is feed back for next stage (hence name)
- standard allows any number of bits (1,8, 64 or 128 etc) to be feed back
  - denoted CFB-1, CFB-8, CFB-64, CFB-128, etc.
- most efficient to use all bits in block (64 or 128)

$$C_i = P_i \text{ XOR } E_K(C_{i-1})$$

$$C_{-1} = IV$$

- uses: stream data encryption, authentication

s-bit Cipher FeedBack (CFB-s)



Advantages and Limitations of CFB

- most common stream mode
- appropriate when data arrives in bits/bytes
- note that the block cipher is used in **encryption** mode at **both** ends (XOR)
- errors in one or more bits of the ciphertext block affects the next ciphertext blocks.

Output FeedBack (OFB)

- message is treated as a stream of bits
- The output of the encryption function is fed back to the shift register.(hence name)

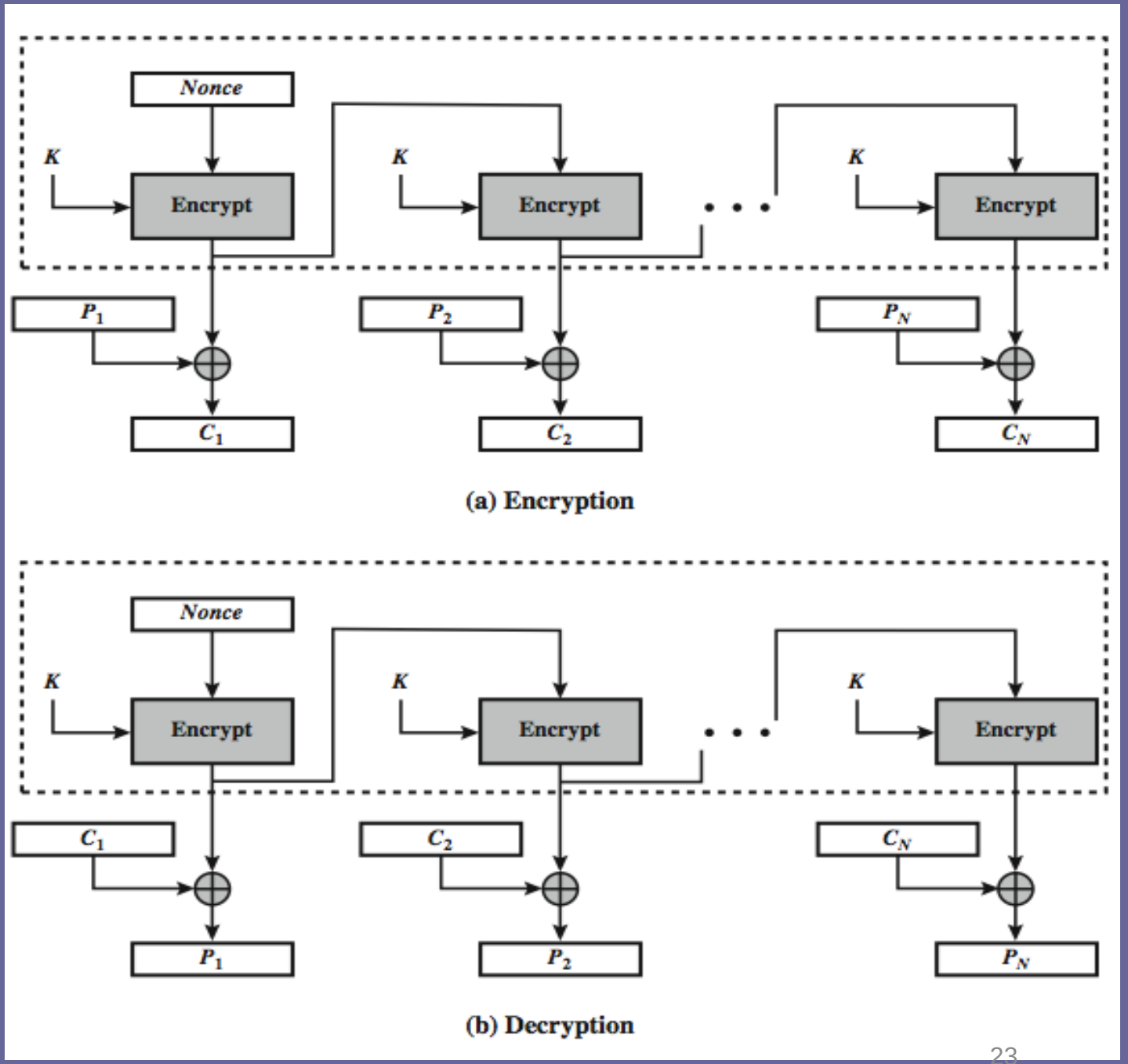
$$O_i = E_K(O_{i-1})$$

$$C_i = P_i \text{ XOR } O_i$$

$$O_{-1} = IV$$

- feedback is independent of message.

Output FeedBack (OFB)



Advantages and Limitations of OFB

- uses: stream encryption on noisy channels

  Why noisy channels?

Bit errors in transmission do not propagate-If a bit error due to noise in noisy channels occurs in C_1 only the recovered value of P_1 is affected, subsequent plaintext units are not corrupted.

Counter (CTR)

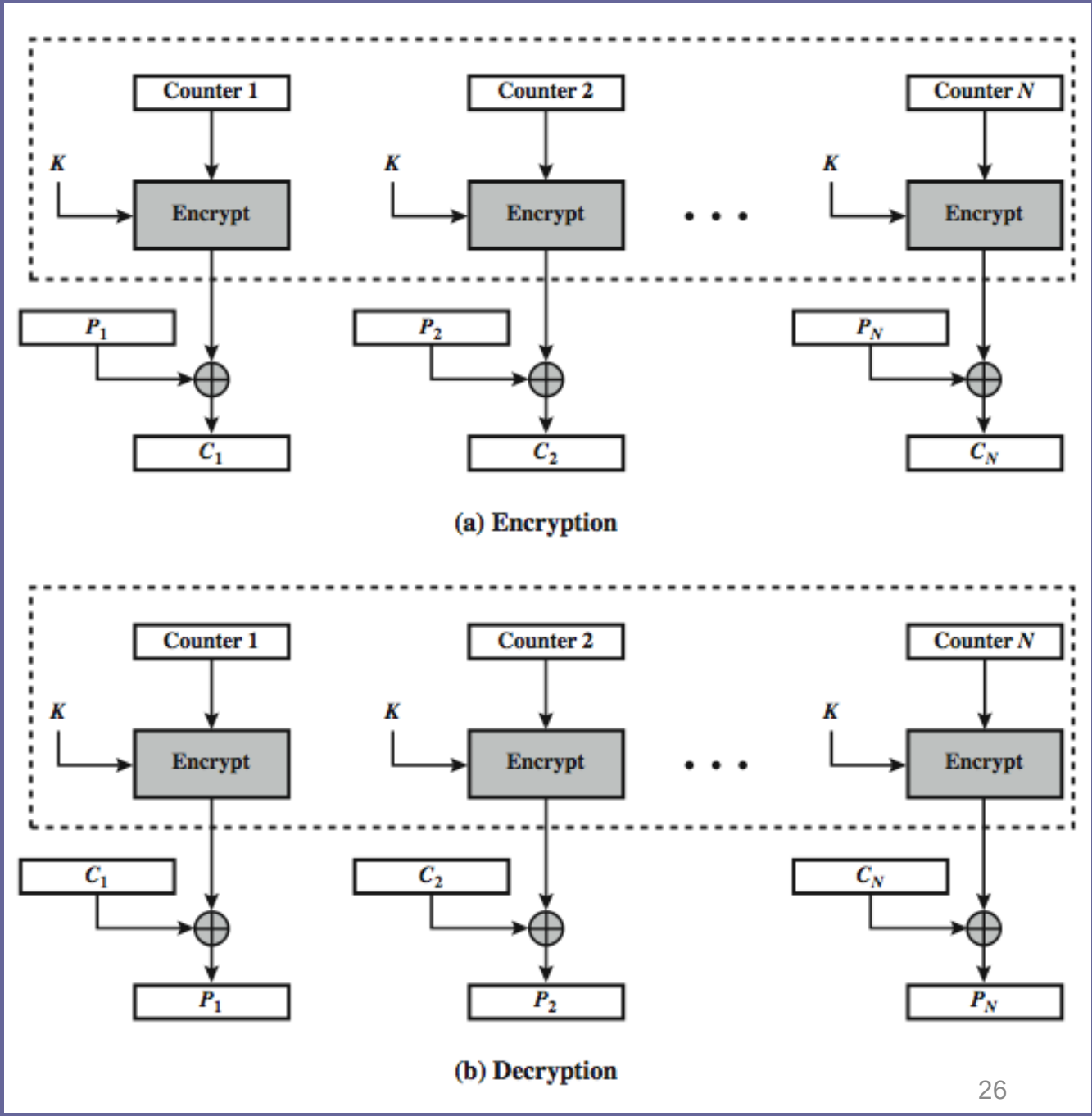
- a “new” mode, though proposed early on
- similar to OFB but encrypts counter value rather than any feedback value

$$O_i = E_K(i)$$

$$C_i = P_i \text{ XOR } O_i$$

- must have a different key & counter value for every plaintext block (never reused)
- uses: high-speed network encryptions
- can do parallel encryptions.

Counter (CTR)


Counter 1
Counter 2
Counter N
K
Encrypt
P_1
P_2
P_N
C_1
C_2
C_N
(a) Encryption
(b) Decryption

Feedback Characteristics